AMENDMENTS

In the Specification:

Page 5, lines 1-7, amend the paragraph as follows:

As shown in Fig. 1, the four-corner model preferably comprises a first institution 102 and a second institution 104. First institution 102 is referred to as the "issuing [[_]]participant" because it is a participant in the present system and issues smart cards to its customers, as described below. Second institution 104 is referred to as the "relying participant" because it is a participant in the present system and its customers rely on representations made by issuing participant 102 and issuing participant 102's customers, as described below. Participants 102, 104 are typically banks or other financial institutions.

Page 5, lines 29-35 to Page 6, lines 1-5, amend the paragraph as follows:

Fig. 2 is a block diagram depicting components preferably provided at each entity in the four corner model. As shown in Fig. 2, participants 102, 104, and root entity 110 are each preferably provided with a transaction coordinator 202 that serves as a gateway for transmitting and receiving all inter-entity messages related to services provided by the present system. Each transaction coordinator 202 is preferably provided with an associated hardware security module (HSM) 218 for signing and verifying messages. Transaction coordinators 202 provide a single interface to issuing participant 102's and relying participant 104's on-line services and implement safeguards necessary to ensure secure electronic communications between transaction coordinators 202 and other entities in the four-corner model, as described in copending United States patent application serial No. [[_____]], 09/657,605 filed on ~~even date herewith~~ September 8, 2000, entitled System and Method for Providing Certificate Validation and Other Services, which is hereby incorporated by reference.

Page 6, lines 14-19, amend the paragraph as follows:

Other components shown in Fig. 2 as well as exemplary services and message flows for such services are described in copending United States patent application serial No.[[_____]]

09/657,621 filed on ~~even date herewith~~ September 8, 2000, entitled System and Method for Providing Certificate Validation and Other Services and United States patent application serial No. [[_____]] 09/657,622 filed on ~~even date herewith~~ September 8, 2000, entitled System and Method for Providing Payment Services in Electronic Commerce.

Page 7, lines 1-10, amend the paragraph as follows:

In a preferred embodiment, subscribing customer 106's digital certificates and associated private keys are provided to it by issuing participant 102. Issuing participant 102 preferably issues smart cards or other suitable instruments to subscribing customer 106 that include at least the private key associated with the subscribing customer's identity certificate. If desired, the smart card may also include the subscribing customer's identity certificate. Preferred specifications for the smart card, its manufacture, and contents are described in copending United States provisional patent application serial No.[[_____]] 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service Functional Requirements, and Additional Disclosure, which is hereby incorporated by reference.

Page 8, lines 3-9, amend the paragraph as follows:

Preferred embodiments for implementing this signing interface are described in copending United States provisional patent application serial No.[[_____]] 60/224,994, filed August 14, 2000, entitled Signing Interface Requirements, Smart Card Compliance Requirements, Warranty Service Functional Requirements, and Additional Disclosure, which is hereby incorporated by reference. As disclosed therein, in one preferred embodiment this signing interface may be implemented using a ~~Java~~ JAVA applet downloaded from the customer seller's Web server to the buyer's Web browser.

Page 8, lines 10-16, amend the paragraph as follows:

Using a ~~Java~~ JAVA applet to implement the client interface is advantageous for several reasons. First, the applet can be automatically downloaded from the server each time it is used; therefore, no additional software is required on the signer's machine to support PKI integration (except for the drivers necessary for smart card access) and the applet can be updated without client distribution requirements. Second, ~~Java~~ JAVA is a cross-platform technology and therefore use of a ~~Java~~ JAVA applet allows the system to support all ~~Java~~ JAVA compliant browsers. Third, the OpenCard API provides smart card access from ~~Java~~ JAVA.

Page 8, lines 17-24, amend the paragraph as follows:

In a second preferred embodiment, data signing may be handled by a series of browser plug-ins. For example, GENERAL NETWORK SOLUTIONS ~~General Network Solutions (http://www.gns.ca/)~~ provides a set of browser plug-ins called FormSign that may be used to sign a form's posted data. In this preferred embodiment, one or more plug-ins are installed on the client's machine before signing occurs. A plug-in may, for example, be downloaded over the Internet to the client's computer the first time the user receives a page referencing; it. Plug-ins provide a good solution for active integration where the HTML page to be signed can be modified to explicitly reference the plug-in.

Page 8, lines 25-33, amend the paragraph as follows:

The signed data and buyer's certificate are passed back to filter engine 306 which then determines whether a system service is required. For example, the seller may wish to validate the buyer's certificate. In that event, filter engine 306 transmits a message to bank interface 222 which formulates a formal OCSP request and transmits it to transaction coordinator 202_{RP} of relying participant 104. An OCSP response is generated as described 30 in more detail in copending United States patent application serial No. [[_____]] 09/657,621 filed on ~~even date herewith~~ September 8, 2000, entitled System and Method

for Providing Certificate Validation and Other Services, which is hereby incorporated by reference, and returned to bank interface 222, which forwards the response to filter engine 306.

Page 9, lines 5-7, amend the paragraph as follows:

Thus, an important attribute of passive integration is that SDK Web server 312 receives all incoming connections previously destined for Web server 220. Few changes to original Web server ~~312~~ 220 are needed, except that it is no longer accessible from the Internet. Additionally, existing certificates used for SSL encryption may need to be reconfigured to use SDK Web server 312.

Page 9, lines 12-15, amend the paragraph as follows:

A computer platform for implementing Web server 312 preferably contains a minimum of 128 Mb of random access memory and a 10 Mb hard disk. In a preferred embodiment, the system may be implemented on the MICROSOFT WINDOWS NT ~~Microsoft Windows NT~~ platform, with the following recommended configuration.

Page 9, lines 16-35 to Page 10, lines 1-2, delete table.

Page 10, lines 4-7, amend the paragraph as follows:

In a preferred embodiment, ~~Java~~ JAVA is used as a language/platform and is compiled to an intermediate format called byte codes. These byte codes are then executed by a virtual machine. If a ~~Java~~ JAVA Virtual Machine (JVM) is available for the target platform, the ~~Java~~ JAVA code can be executed on that platform

Page 11, lines 1-9, amend the paragraph as follows:

A number of ISA technologies exist; some are specific to one Web server and others are-industry-standards supported by most major Web servers. Because the present-system preferably supports many

Web server and platform combinations, a ~~Java~~ JAVA implementation is preferred for implementing this ISA. Servlet technology is based on ~~Java~~ JAVA and is supported by several commercially available Web servers through third-party servlet engines. In a preferred embodiment, servlet 304 may be implemented using ~~Live Software's Jrun 2.2~~ LIVE SOFTWARE'S JRUN 2.2 product ~~(http://www.irun.com/),~~ a servlet engine that provides integration with several commercially available Web servers, including ~~Microsoft Internet Information Server~~ MICROSOFT INTERNET INFORMATION SERVER ("IIS"), ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER ("NES"), and ~~Apache~~ APACHE.

Page 11, lines 10-21, amend the paragraph as follows:

Performance issues with servlets, however, may drive a decision to implement other ISA technologies. For example, in an alternative preferred embodiment, the functionality of servlet 304 may instead be provided by an Internet Server Application Programming Interface (ISAPI). ISAPI is a C-based ISA developed for ~~Microsoft Internet Information Server~~ MICROSOFT INTERNET INFORMATION SERVER (US). A port of ISAPI has been done for the ~~Apache~~ APACHE Web server as well. The corresponding, but different, ISA technology for ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER (NES) is ~~Netscape Server Application Programming Interface~~ NETSCAPE SERVER APPLICATION PROGRAMMING INTERFACE (NSAPI). These two interfaces provide close, C-based support for their respective Web servers and therefore provide maximum performance. The problem with using these C-based technologies is the number of platform and Web server combinations that must be written to cover the same breadth as a servlet. Thus, although servlets are typically preferred, ISAPI and NSAPI extensions may be written as necessary for select platforms to improve performance.

Page 15, lines 20-21, amend the paragraph as follows:

In a preferred embodiment, filter engine 306 provides an abstracted front-end interface via ~~Java~~ JAVA Remote Method Invocation (RMI).

Page 15, lines 22-26, amend the paragraph as follows:

In a preferred embodiment, filter engine 306 may be implemented as a public class object that extends java.lang.Object. This class implements one of the public services provided by filter engine 306's RMI server. —— Illustrative methods for this object are shown and described in the table below. Methods inherited from the parent class java.lang.object are not shown in the table.

Page 25, lines 17-22, amend the paragraph as follows:

1. Conform XML requests to a messaging set defined by root entity 110. An exemplary messaging set is described in copending United States provisional patent application serial No. [[_____]] 60/231,319, filed on ~~even date herewith~~ September 8, 2000, entitled Transaction Coordinator Certificate Status Check (CSC) Protocol Definition, Transaction Coordinator Messaging Protocol Definition.

Page 26, lines 9-16, amend the paragraph as follows:

In an alternative preferred embodiment, rather than supporting both raw OCSP and OCSP wrapped in XML, the system may employ a pure XML implementation. Standards based protocols for certification validation may also be considered rather than devising a new proprietary protocol. One such protocol is the "Simple Certificate Validation Protocol (SCVP)" which is in an Internet-draft form at the current time. This protocol would enable a relying customer 108 to offload path validation responsibilities to a remote path processing server (RPPS). ~~More information about this protocol may be found at the IETF web site http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-02.txt.~~